Joint Personnel Adjudication System (JPAS) Overview

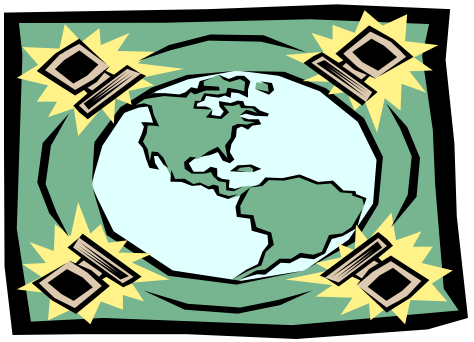
DSSAcademy
Security Through Knowledge

Important

- **This overview addresses information and instructions on the use of the Joint Personnel Adjudication System (JPAS).**
- **It is an instructional tool only and is not meant to dictate policy.**
- **Future enhancements will be announced on the JPAS website at https://jpas.dsis.dod.mil.**

JPAS

- **The Department of Defense (DoD) system that uses the Web to connect security personnel around the world with a database managed by DoD Agency Central Adjudication Facilities (CAFs)**



- **Represents a major technological leap for DoD personnel security professionals worldwide**

JPAS

The DoD personnel security migration system:

- **Providing the virtual consolidation of the DoD CAFs**
- **For use by non-SCI security program managers, Special Security Officers, and DoD contractor security officers**
- **Uses a centralized database with centralized computer processing and application programs for standardized DoD personnel security processes**

JPAS

Provides "real-time" information regarding clearance, access and investigative status to authorized DoD security personnel and other interfacing organizations such as the:

Defense Security Service
Defense Manpower Data Center
Defense Civilian Personnel Management System
Office of Personnel Management

JPAS

- **Comprised of two major sub systems:**
  - **the Joint Clearance and Access Verification System (JCAVS)**
  - **the Joint Adjudication Management System (JAMS)**

JCAVS + JAMS = JPAS

JCAVS

- **Provides ability to constantly update accesses and related information in real time**

- **Provides ability to constantly communicate with other information systems:**

  - **DSS, OPM, DEERS, DCPMS, Bupers (USN), MCTFS (Marines)**

JAMS

- **Provides DoD CAFs a single information system to assist in the adjudication process**
- **Standardizes core DoD Adjudication processes**
- **Used by Adjudicators to record eligibility determinations and command access decisions**

Vocabulary

- **JPAS speaks in terms of eligibility and access instead of personnel security clearance**
- **The government continues to issue eligibility to an individual**
- **The security officer assigns**

Definitions

- **Eligibility**
  - **the highest level of information which may be disclosed to a person based on the type of completed investigation**
  - **CAF Responsibility**
- **Access**
  - **the actual level of classified information to which a person is authorized disclosure**

JCAVS User Levels

- **Total 12**
  - **Levels 9,11,12 are not yet defined**
  - **Level 10 = Visit Control Only**

JCAVS

- **Level 2**

  - **SCI security personnel at unified command, DoD agency, military department or major command/equivalent headquarters**

  - **For industry - usually the Chief Security Officer at the corporate level, Special Security Officer (SSO or CSSO)**

  - **Provides Read and Write Access**

JCAVS

- **Level 3**
  - **SCI security personnel subordinate to Level 2 at a particular geographic location (installation, base, post, naval vessel or facility)**
  - **Provides Read and Write Access**
  - **Requires an SSBI with DCID eligibility and access**

JCAVS

- **Level 4**
  - **Non-SCI security personnel at unified command, DoD agency, military department or major command/equivalent headquarters**
  - **For industry - Corporate FSOs (collateral)**
  - **Provides Read and Write Access**

JCAVS

- **Level 5**
  - **Non-SCI security personnel subordinate to Level 4 at a particular geographic location (installation, base, post, naval vessel)**
  - **For Industry - Company FSOs / Managers (collateral)**
  - **Provides Read and Write Access**

JCAVS

- **Level 6**
  - **Unit security manager (additional duty) responsible for security functions as determined by responsible senior security official**
  - **For industry - Unit Security Managers / Visitor Control**
  - **Provides Read and Write Access**

JCAVS

- **Level 7**
  - **Non-SCI entry control personnel / individuals who grant access to installations, buildings, etc.**
  - **For industry - lobby receptionists, security entry point personnel (collateral)**
  - **Provides Read Only Access**

JCAVS

- **Level 8**
  - **SCI entry control personnel / individuals who grant access to Sensitive Compartmented Information Facility (SCIF) installations, buildings, etc.**
  - **For industry - lobby receptionist, security entry point (SCI)**
  - **Provides Read Only Access**

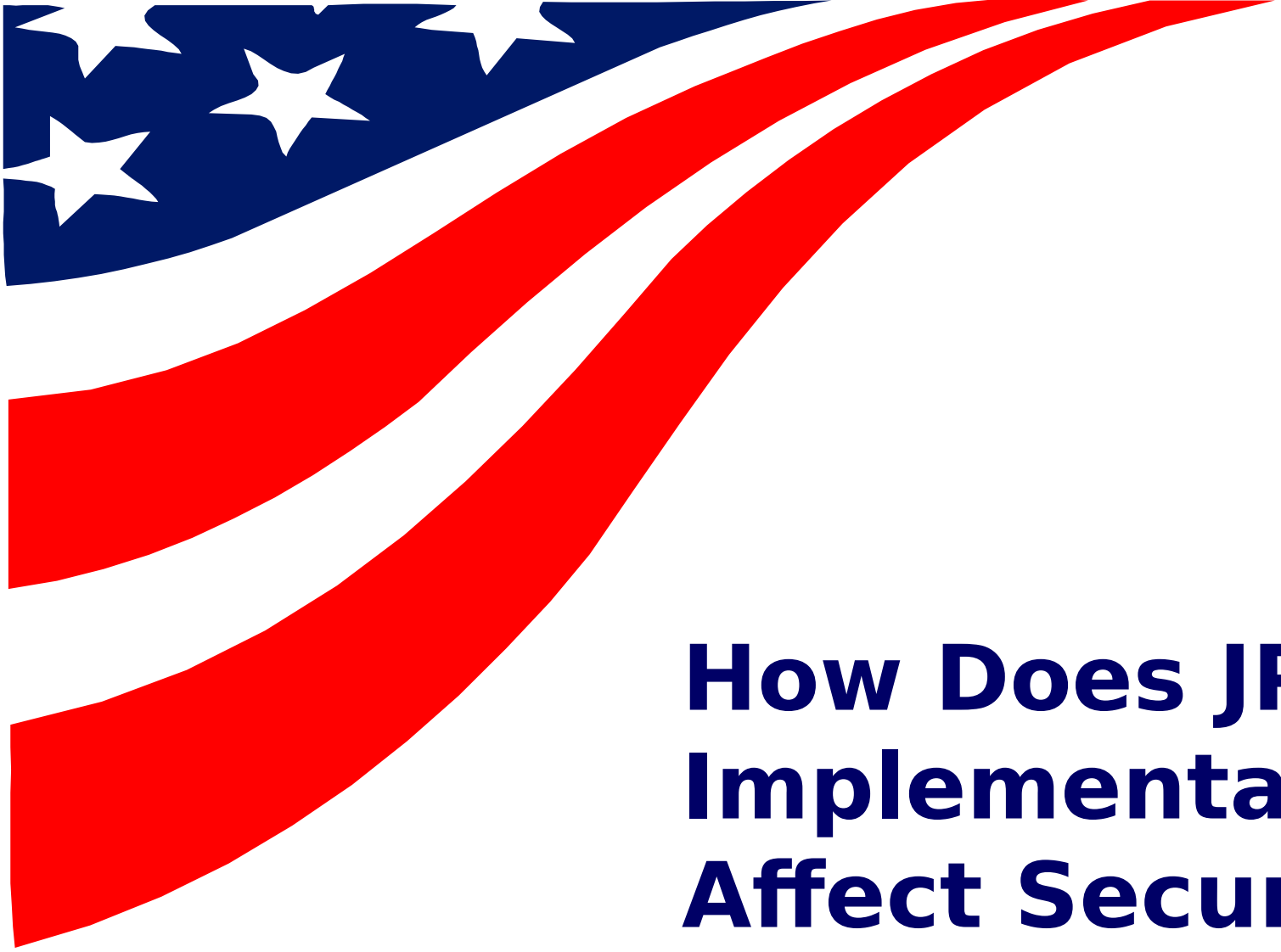
JCAVS

- **Level 10**
  - **Visitor management personnel**
  - **Has the same view of the JCAVS Person Summary as a JCAVS Level 7 User**
  - **Receives Visit Notifications when their Security Management Office (SMO) is being notified of a visit**

User Investigative Requirements

- **Levels 2, 3 and 8 – Current SSBI**
- **Levels 4 – 7 and 10 – NACLC with Credit***

***If projected user has a NAC without c**
a new EPSQ will be required with reas
listed as “Requires access to JPAS.”



How Does JPAS Implementation Affect Security Office Operations?

Security Officers

- **Must now speak JPAS**
  - **Remember Eligibility and Access replace Personnel Security Clearance**

- **Assigns the individual's access level in JCAVS**

Access
Eligibility
Authorize
d Person
Need-
to-
Know

Record Keeping

- **JPAS automates core and CAF-unique functionality and provides "real-time" eligibility, access and investigative status to DoD and other interfacing organizations**

- **JCAVS will automatically record “eligibility” at the highest level commensurate with the level of investigation**

NOW
Security Officers Can:

- Grant access based on JPAS record of eligibility
- Upgrade level of access immediately
- Downgrade level of access immediately
- Terminate access immediately
- Record SF 312 execution (Once!)
- Send U.S. Visits
- In/Out-Process employees / verify eligibility
- Submit Incident (formally known as

System Access Requirements

- **Desktop configuration**
- **.com, .mil, .gov, .org, or .net address**

  .net or .org addresses must identify their specific IP address to the JPAS helpdesk

Designation of Users

- **Two Functional Categories**
  - **JCAVS Account Manager**
  - **JCAVS User**

- **Account Level dependent on:**
  - **Facility or command clearance level**
  - **Requirement to SCI or non-SCI eligibility and access data**

Account Manager

- **Responsible for JPAS compliance**
- **First line of assistance on-site – the organization's "help desk"**
- **Creates a Security Management Office**

  Inputs Security Officer's name, e-mail,
  phone and fax numbers

Account Manager

- **Performs administrator functions such as:**
  - **Issuance of User ID and passwords**
  - **Re-setting passwords**
  - **Locking / un-locking user accounts**
  - **Changing user account privileges**
  - **Point of contact for system technical issues**

Account Manager

- **Examples of accountable actions:**
  - **Identify who has been given JCAVS accounts and at what level**
  - **Produce Access Request Forms for review**
  - **Track JCAVS accounts that has been terminated, or where privileges have been suspended**

Functional User

- **Typically the Security Officer or designee**
- **Uses the system on a regular basis to verify eligibility, investigations, send visit requests, maintain personnel security records, etc.**

JPAS

- **For additional questions, clarification and/or points of contact, please access the JPAS website:**
  https://jpas.dsis.dod.mil

- **E-mail: JPASHD@dss.mil**

- **Or call the DoD Security Service Center:**

  1-888-282-7682